

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

Money and Data Protection Lizenz
GMPH & Co. KG,

Plaintiff,

v.

Duo Security, Inc.,

Defendant.

Civil Action No. 18-1477-CFC

Stefan Mentzer, Leon Miniovich, Scott T. Weingaertner, WHITE & CASE LLP,
New York, New York; Stephanie E. O'Byrne, David E. Moore, Bindu A. Palapura,
POTTER ANDERSON & CORROON LLP, Wilmington, Delaware


Counsel for Plaintiff

Justin M. Barnes, Elizabeth R. Brannen, STRIS & MAHER LLP, Los Angeles,
California; Jack B. Blumenfeld, Jennifer Ying, MORRIS, NICHOLS, ARSHT &
TUNNELL LLP, Wilmington, Delaware

Counsel for Defendant

MEMORANDUM OPINION

June 24, 2020
Wilmington, Delaware


COLM F. CONNOLLY
UNITED STATES DISTRICT JUDGE

Plaintiff Money and Data Protection Lizenz GMPH & Co. KG (MDPL) has sued Defendant Duo Security, Inc. for infringement of U.S. Patent No. 9,246,903 (the #903 patent). D.I. 15. MDPL filed its Amended Complaint in September 2019. *Id.* Duo filed an answer to the Amended Complaint in October 2019. D.I. 16. Pending before me is Duo's motion for judgment on the pleadings pursuant to Federal Rule of Civil Procedure 12(c). D.I. 17. Duo argues that judgment in its favor is warranted because all claims of the #903 patent are invalid under 35 U.S.C. § 101 for failing to claim patentable subject matter.

I. BACKGROUND¹

The #903 patent is directed to the authentication (i.e., verification) of the identification of the user of a device or terminal to conduct a transaction. The patent's written description makes note of an obvious reality of our "virtual" world: "In transactions in which a user communicates with a remote transaction partner via a communication channel such as the Internet, it is important to assure that an individual that identifies itself as an authorised user is actually the person it

¹ When assessing the merits of a Rule 12(c) motion for judgment on the pleadings, I accept as true all factual allegations in the pleadings and view those facts in the light most favorable to the Plaintiff. *See Zimmerman v. Corbett*, 873 F.3d 414, 417–18 (3d Cir. 2017) (citations omitted).

alleges to be.” #903 Patent at 1:15–19. The patent purports to teach a method that “assures that no third party can fake the identification data of [a] user and perform any transactions in his place.” *Id.* 1:51–53.

Claim 1 is the only independent claim in the #903 patent, and MDPL contended in its original complaint that Claim 1 was “exemplary” of the #903 patent’s claims. D.I. 1 ¶ 13. Claim 1 reads as follows:

A method of authenticating a user to a transaction at a terminal, comprising the steps of:

transmitting a user identification from the terminal to a transaction partner via a first communication channel,

providing an authentication step in which an authentication device uses a second communication channel for checking an authentication function that is implemented in a mobile device of the user,

as a criterion for deciding whether the authentication to the transaction shall be granted or denied, having the authentication device check whether a predetermined time relation exists between the transmission of the user

identification and a response from the second communication channel,

ensuring that the authentication function is normally inactive and is activated by the user only preliminarily for the transaction,

ensuring that said response from the second communication channel includes information that the authentication function is active, and

thereafter ensuring that the authentication function is automatically deactivated.

#903 patent at 10:39–60.

II. LEGAL STANDARDS

A. Motion for Judgment on the Pleadings

“The purpose of judgment on the pleadings is to dispose of claims where the material facts are undisputed and judgment can be entered on the competing pleadings and exhibits thereto, and documents incorporated by reference.” *Int’l Bus. Machines Corp. v. Groupon, Inc.*, 289 F. Supp. 3d 596, 600 (D. Del. 2017) (citations omitted). “A motion for judgment on the pleadings should be granted if the movant establishes that there are no material issues of fact, and [the movant] is entitled to judgment as a matter of law.” *Zimmerman v. Corbett*, 873 F.3d 414, 417 (3d Cir. 2017) (internal quotation marks and citations omitted). “In considering a motion for judgment on the pleadings, a court must accept all of the allegations in the pleadings of the party against whom the motion is addressed as true and draw all reasonable inferences in favor of the non-moving party.” *Id.* at 417–18 (citations omitted).

B. Patent-Eligible Subject Matter

Section 101 of the Patent Act defines patent-eligible subject matter. It provides: “Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of

this title.” 35 U.S.C. § 101.

There are three judicially created limitations on the literal words of § 101. The Supreme Court has long held that laws of nature, natural phenomena, and abstract ideas are not patentable subject matter. *Alice Corp. Pty. v. CLS Bank Int’l*, 573 U.S. 208, 216 (2014). These exceptions to patentable subject matter arise from the concern that the monopolization of “the[se] basic tools of scientific and technological work” “might tend to impede innovation more than it would tend to promote it.” *Id.* (internal quotation marks and citations omitted).

“[A]n invention is not rendered ineligible for patent [protection] simply because it involves an abstract concept.” *Alice*, 573 U.S. at 217. “Applications of such concepts to a new and useful end . . . remain eligible for patent protection.” *Id.* (internal quotation marks, alterations, and citations omitted). But “to transform an unpatentable law of nature [or abstract idea] into a patent-eligible application of such a law [or abstract idea], one must do more than simply state the law of nature [or abstract idea] while adding the words ‘apply it.’” *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 72 (2012) (emphasis removed).

In *Alice*, the Supreme Court established a two-step framework by which courts are to distinguish patents that claim eligible subject matter under § 101 from patents that do not claim eligible subject matter under § 101. The court must first determine whether the patent’s claims are drawn to a patent-ineligible concept—

i.e., are the claims directed to a law of nature, natural phenomenon, or abstract idea? *Alice*, 573 U.S. at 217. If the answer to this question is no, then the patent is not invalid for teaching ineligible subject matter. If the answer to this question is yes, then the court must proceed to step two, where it considers “the elements of each claim both individually and as an ordered combination” to determine if there is an “inventive concept—*i.e.*, an element or combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.” *Id.* at 217–18 (alteration in original) (internal quotations and citations omitted).

III. DISCUSSION

I agree with Duo that the #903 patent’s claims are directed to the abstract idea of authentication—that is, the verification of identity to permit access to transactions. The #903 patent is not materially different from the patent at issue in *Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App’x 1014 (Fed. Cir. 2017). The Federal Circuit determined that the patent in *Prism* was invalid because it was directed to the abstract idea of “providing restricted access to resources.” *Id.* at 1016–17. The claims of the patent in *Prism* taught “an abstract process” that included: “(1) receiving identity data from a device with a request for access to resources; (2) confirming the authenticity of the identity data associated with that device; (3) determining whether the device identified is authorized to access the

resources requested; and (4) if authorized, permitting access to the requested resources.” *Id.* The #903 patent’s authentication method closely parallels this abstract process. In the method claimed by the #903 patent, a user inputs identification information into a first communication channel to request access to a transaction. *See* #903 patent at 10:39–42. An authentication device then confirms the user’s identity by using a second communication channel to check that an authentication function has been implemented on the user’s mobile device. *See id.* at 10:43–46. The authentication device then follows several criteria to check whether the response from the second communication channel is authorized before approving the transaction. *See id.* at 10:47–60. Given the similarities between the abstract processes in the #903 patent and the patent in *Prism*, I find that the claims at issue here are directed to the abstract idea of verifying identity to permit access to transactions.

Turning, then, to the second step of the *Alice* analysis, the question is whether the #903 patent claims an inventive concept sufficient to ensure that the patent in practice teaches significantly more than the mere verification of identity to permit access to transactions. In *Alice*, the Court considered at step two “the introduction of a computer into the claims” and held that “the mere recitation of a generic computer [in the claims] cannot transform a patent-ineligible abstract idea

into a patent-eligible invention.” *Alice*, 573 U.S. at 222–23.² Thus, the use of “a generic computer to perform generic computer functions” does not provide the requisite inventive concept to satisfy step two of the *Alice* analysis. *Id.* at 225.

In this case, the #903 patent merely teaches generic computer functionality to perform the abstract concept of authentication; and it therefore fails *Alice*’s step two inquiry. Claim 1 of the #903 patent recites the following claim elements: a terminal, *see* #903 patent at 10:40; first and second communication channels, *see id.* at 10:42; *see also id.* at 10:44; an authentication device, *see id.* at 10:43–44; an authentication function, *see id.* at 10:45; a mobile device, *see id.* at 10:46; and a predetermined time relation, *see id.* at 10:49–50. The patent describes these individual elements as performing their conventional functions at each step of the method. *See id.* at 2:35–38 (noting that a terminal may be “a banking machine or a cashier . . . but may also be any other device, such as a computer, capable of communicating with a remote transaction partner”); *see id.* at 4:39–45 (noting that a first communication channel “may be a wireline or wireless channel” and a second communication channel “preferably includes a wireless link, e.g. a mobile telephone network”); *see id.* at 1:30–46 (noting that the prior art employed

² *But see Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335–36 (Fed. Cir. 2016) (considering introduction of computer functionality into claims as part of step one of *Alice* inquiry); *see also In re TLI Commc’ns LLC Patent Litig.*, 823 F.3d 607, 611–13 (Fed. Cir. 2016) (same).

authentication devices, authentication functions, and mobile devices to carry out authentication methods); *see id.* at 1:54–56 (noting that users may employ mobile devices of “low complexity” to implement the authentication method); *see id.* at 1:30–34 (discussing GB 2 398 159 A, a prior art authentication method that prompts a user to send a confirmatory message within a predetermined time period to complete the transaction).

Considered individually and as an ordered combination, the claim elements of the #903 patent teach no more than the performance of “well-understood, routine, and conventional activities previously known to the industry.” *Alice*, 573 U.S. at 225 (internal quotation marks and citation omitted). The #903 patent discusses several prior art authentication methods that employed mobile devices to verify a user’s identity to an Internet transaction. *See, e.g.*, #903 patent at 1:15–53. And the only purported difference between those prior art methods and the claimed invention is that the #903 patent’s method “can be carried out with mobile devices of low complexity” so that “all that has to be required from the authentication function is to permit the authentication device to detect whether or not this function is active. . . . [and] the only activity that is required from the user for authentication purposes is to activate the authentication function at a suitable timing for the transaction.” *Id.* at 1:55–2:3. But as the patent itself discloses, the detection of an authentication function’s activity and the activation by users of an authentication

function within a pre-determined time relation were well-understood and routine, conventional activities previously known in the authentication technology field.

See id. at 1:15–53. “Purely ‘conventional or obvious’ ‘[pre]-solution activity’ is . . . not sufficient to transform an unpatentable law of nature into a patent-eligible application of such a law.” *Mayo*, 566 U.S. at 79 (citations omitted).³

MDPL argues that the claimed invention is patentable under § 101 because it “improves computer-related technology by increasing the efficiency of a networked authentication process, saving cost, and relieving much of the burden on the user.” D.I. 20 at 6. According to MDPL, “the ’903 patent claims a specific improvement to a particular authentication technique rooted in computer technology.” *Id.* at 2. MDPL describes this “specific improvement” as follows:

Rather than requiring the user to retrieve information and input multiple authentication factors, the user’s identity is verified by (1) transmitting the user identification, such as a username, via a first communication channel, and (2)

³ MDPL contends that “[t]he question of whether that improvement was ‘well-understood, routine, and conventional[.]’ to a skilled artisan in the relevant field is a question of fact” that is not suitable for a motion for judgment on the pleadings. D.I. 20 at 18. But there are no facts alleged in the Amended Complaint that demonstrate how the invention claimed by the #903 patent improves authentication technology, and, as discussed above, the #903 patent itself does not disclose how the claimed authentication method differs from—much less improves upon—the authentication methods used in the prior art. On the contrary, the patent’s written description makes clear that the inventor intended to implement existing authentication methods on “mobile devices of low complexity” using well-known authentication functions, *see* #903 patent at 1:15–53, and pre-determined time relations, *see id.* at 1:30–34.

checking via a second communication channel that an authentication function is activated in the user's mobile device. By replacing manual entry of information for an authentication factor with a check for an activated authentication function, the '903 patent provides a more efficient system. For example, to activate the authentication function, the user may simply activate their mobile device, activate an app on a smartphone, or flip a switch on a key fob.

Id. at 2–3 (citations omitted). MDPL contends that this method “cannot be performed by hand or with technologies much older than computers” because “[i]t is not possible for a person to mentally or manually check for an activated authentication function in a mobile device over a second communication channel[.]” *Id.* at 15.

But it is possible for a person “to mentally or manually” obtain activation information in a register or database, and the #903 patent discloses that checking for an activated authentication function is accomplished in precisely that manner—i.e., by obtaining the device's identifier, location, and state-of-activation information from a mobile network Home Location Register (HLR). #903 patent at 2:44–67. The patent does not teach a technical solution that enables a computer to access an HLR; rather it teaches simply the idea of data gathering from an HLR. That type of data collection is a mental process that a person can perform by reading records from a database. It is, in short, an abstract idea that is not patentable.

Contrary to MDPL's assertions, the #903 patent does not claim or teach the improvement of computer technology. The claims in the #903 patent describe a multistep process that authenticates a user to a transaction using a mobile device; they say nothing about changing the functionality of the mobile device. The patent does not describe the problem it purports to solve as being rooted in computer functionality; instead, it states that the inventor's objective was "to provide an authentication method that is easy to handle and can be carried out with mobile devices of low complexity," indicating that the invention merely implements an abstract authentication method on a generic mobile device. *See id.* at 1:54–56.

Finally, and contrary to its description of claim 1 as "exemplary" in its original complaint, MDPL argues that I should not treat claim 1 of the #903 patent as representative because "each dependent claim adds a specific technical element that increases the efficiency of the authentication system." D.I. 20 at 19. Courts, however, may treat a claim as representative where: (i) the claims are "substantially similar and linked to the same abstract idea," *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat. Ass'n*, 776 F.3d 1343, 1348 (Fed. Cir. 2014), and (ii) "the patentee does not present any meaningful argument for the distinctive significance of any claim limitations not found in the representative claim," *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1365 (Fed. Cir. 2018). In this case, the claims are substantially similar and linked to the abstract idea of authentication

and MDPL has not pointed to anything in the dependent claims that distinguish them in any meaningful way from claim 1 with respect to patentability. MDPL discusses in its briefing only dependent claims 4, 5, and 8. Those claims are directed to the same abstract idea as claim 1 and involve the following additional steps: (a) detecting the active state of the authentication function using a communication register of the network (claim 4); and (b) determining the current location of the mobile device (claims 5 and 8). The additional step recited in dependent claim 4 does not add distinctive significance over independent claim 1 because claim 1 already encompasses “ensuring that the authentication function is normally inactive and is activated by the user only preliminarily for the transaction.” #903 patent at 10:53–55. The step of determining the mobile device’s current location in claims 5 and 8 also does not provide distinctive significance over independent claim 1 because claim 1 already provides one “criterion for deciding whether the authentication to the transaction shall be granted or denied”—the “predetermined time relation”; claims 5 and 8 simply add additional criteria the user must meet to complete the transaction. *Id.* at 10:47–50.

IV. CONCLUSION

For the foregoing reasons, I will grant Defendant Duo’s Rule 12(c) Motion for Judgment on the Pleadings for patent invalidity under 35 U.S.C. § 101. D.I. 17.

The Court will issue an Order consistent with this Memorandum Opinion.